HPE6-A81$^{\text{Q\&As}}$

Aruba Certified ClearPass Expert Written Exam

Pass HP HPE6-A81 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

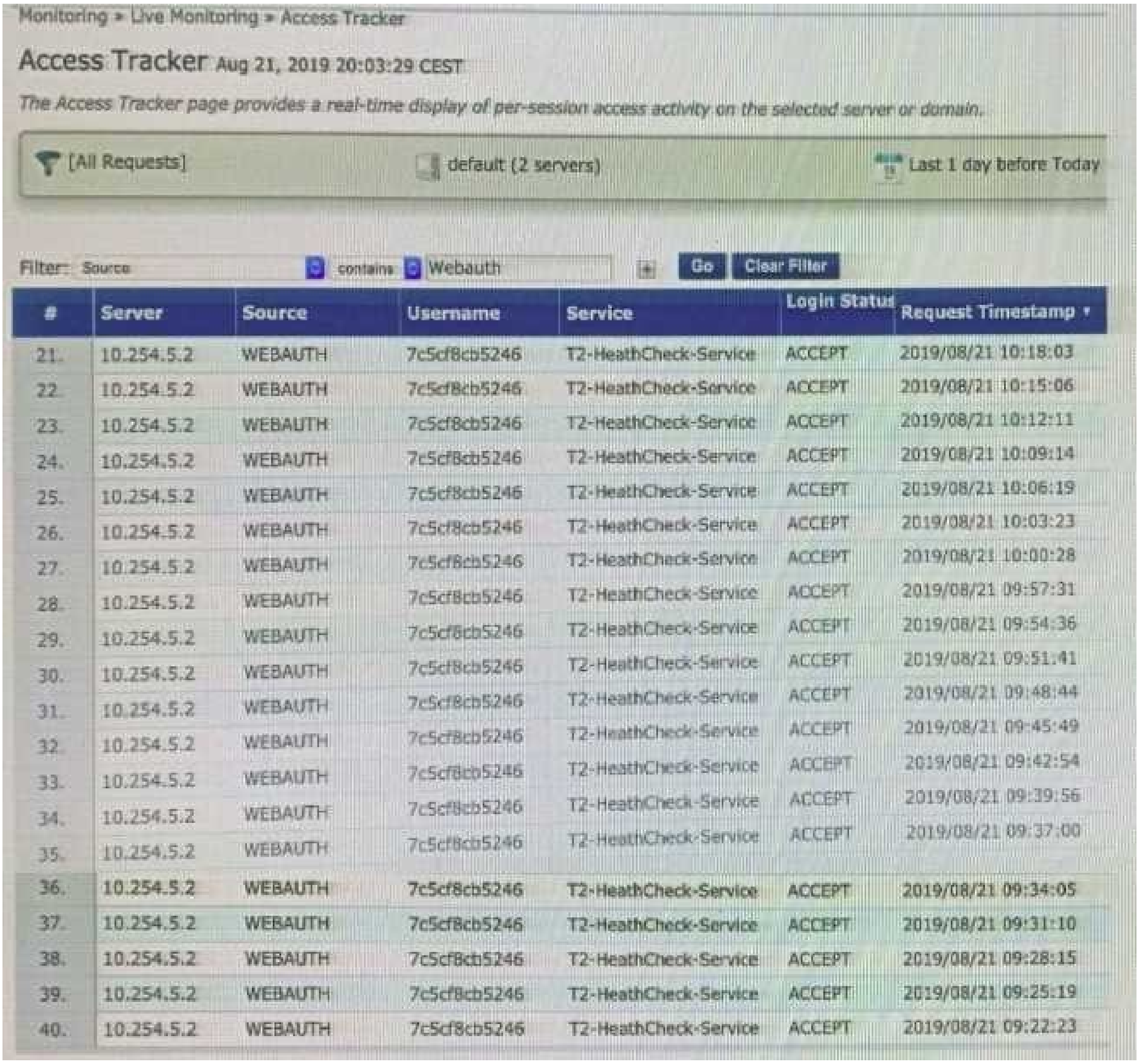
https://www.leads4pass.com/hpe6-a81.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center

QUESTION 1

Refer to the exhibit:



Monitoring » Live Monitoring » Access Tracker

Access Tracker Aug 21, 2019 20:03:29 CEST

The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

[All Requests] default (2 servers) Last 1 day before Today

Filter: Source contains Webauth Go Clear Filter

#	Server	Source	Username	Service	Login Statu	Request Timestamp ▾
21.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 10:18:03
22.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 10:15:06
23.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 10:12:11
24.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 10:09:14
25.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 10:06:19
26.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 10:03:23
27.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 10:00:28
28.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:57:31
29.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:54:36
30.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:51:41
31.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:48:44
32.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:45:49
33.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:42:54
34.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:39:56
35.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:37:00
36.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:34:05
37.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:31:10
38.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:28:15
39.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:25:19
40.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:22:23

A customer has just configured a Posture Policy and the T2-Healthcheck Service. Next they installed the OnGuard Agent on Secure_Employee SSID. When they check Access Tracker they see many WEBAUTH requests are being triggered.

What could be the reason?

A. OnGuard Web-Based Health Check interval has been wrongly configured to three minutes.

B. The OnGuard Agent trigger the events based on changing the Health Status

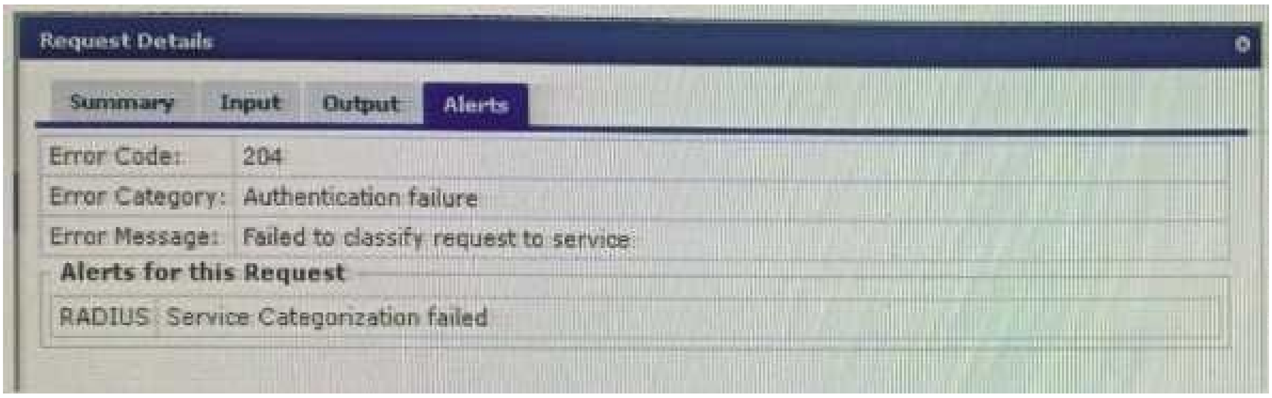
C. TCP port 6658 is not allowed between the client and the ClearPass server

D. The OnGuard Agent is connecting to the Data Port interface on ClearPass

Correct Answer: A

QUESTION 2

Refer to the exhibit: You configured a new Wireless 802.1X service for a Cisco WLC broadcasting the Secure-ADM-5007 SSID. The client falls to connect to the SSID. Using the screenshots as a reference, how would you fix this issue? (Select two.)

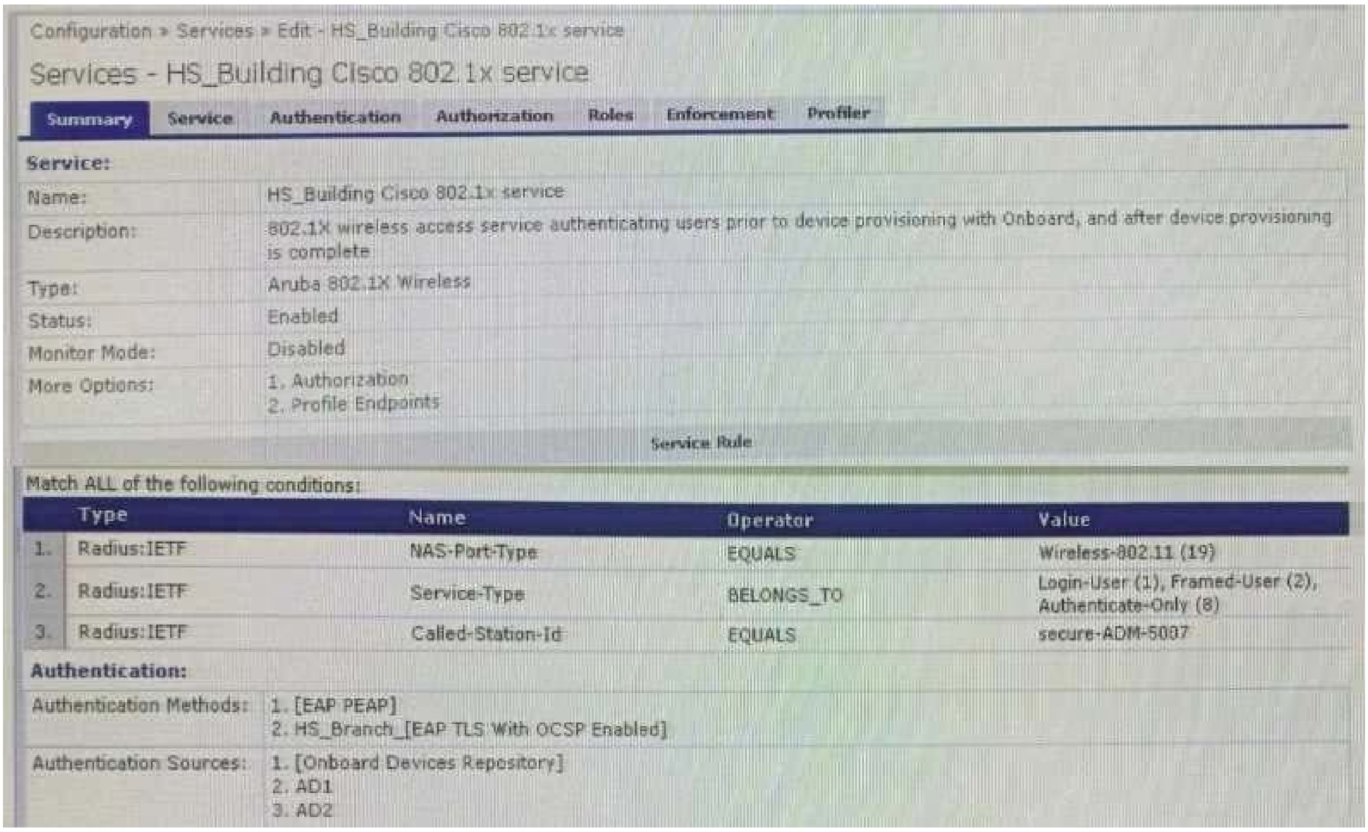


Request Details

Error Code:	204
Error Category:	Authentication failure
Error Message:	Failed to classify request to service

Alerts for this Request

RADIUS	Service Categorization failed



Configuration » Services » Edit - HS_Building Cisco 802.1x service

Services - HS_Building Cisco 802.1x service

Service:

Name:	HS_Building Cisco 802.1x service
Description:	802.1X wireless access service authenticating users prior to device provisioning with Onboard, and after device provisioning is complete
Type:	Aruba 802.1X Wireless
Status:	Enabled
Monitor Mode:	Disabled
More Options:	1. Authorization 2. Profile Endpoints

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3.	Radius:IETF	Called-Station-Id	EQUALS	secure-ADM-5007

Authentication:

Authentication Methods:	1. [EAP PEAP] 2. HS_Branch_[EAP TLS With OCSP Enabled]
Authentication Sources:	1. [Onboard Devices Repository] 2. AD1 3. AD2

A. Update the service condition Radius:IETF Called-Station-ld CONTAINS secure-adm-5007

B. Make sure that the Network Devices entry for the Cisco WLC has a vendor setting of "Airspace"

C. Remove the service condition Radius:lETF Service-Type BELONGSJTO Login-User (1). 2. 8

D. Change the service condition to Radius:lETF Calling-Station-ld EQUALS Secure-ADM-5007

Correct Answer: AC

QUESTION 3

A customer has completed all the required configurations in the Windows server in order for Active Directory Certificate Services (ADCS) to sign Onboard device TLS certificates. The Onboard portal and the Onboard services are also configured. Testing shows that the Client certificates ate still signed by the Onboard Certificate Authority and not ADCS. How can you help the customer with the situation?

A. Educate the customer that, when integrating with Active Directory Certificate Services (ADCS) the Onboard CA will the same authority used for signing me final TLS certificate of the device.

B. Configure the identity certificate signer as Active Directory Certificate Services and enter the ADCS URL http://ADCSVVeoEnrollmentServemostname/certsrv in the OnBoard Provisioning settings.

C. Enable access to EST servers from the Certificate Authority to make ClearPass Onboard to use of the Active Directory Certificate Services (ADCS) web enrollment to sign the device TLS certificates.

D. Enable access to SCEP servers from the Certificate Authority to make ClearPass Onboard to use of the Active Directory Certificate Services (ADCS) web enrollment to sign the device TLS certificates.

Correct Answer: C

QUESTION 4

A customer has configured Onboard with Single SSID provision for Aruba IAP Windows devices work as expected but cannot get the Apple iOS devices to work. The Apple iOS devices automatically get redirected to a blank page and do not get the Onboard portal page. What would you check to fix the issue?

A. Verify if the checkbox "Enable bypassing the Apple Captive Network Assistant" is checked.

B. Verify if the Onboard URL is updated correctly in the external captive portal profile.

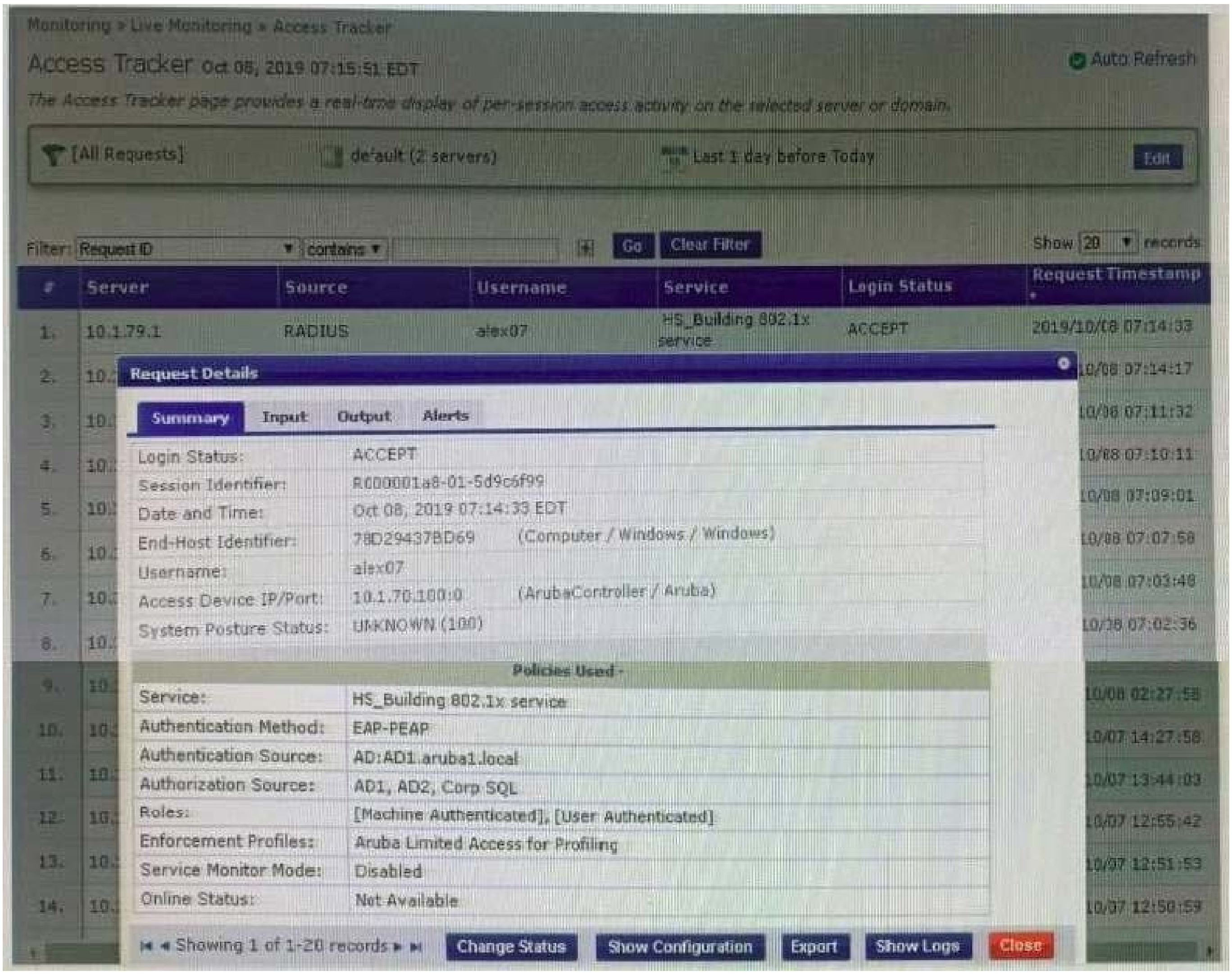
C. Verify if Onboard Pre-Provisioning enforcement profile sends the correct Aruba user role.

D. Verify if the external captive portal profile is enabled to use HTTPS with port 443.

Correct Answer: B

QUESTION 5

Refer to the exhibit:



Access Tracker Oct 08, 2019 07:15:51 EDT

The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

[All Requests] default (2 servers) Last 1 day before Today

Filter: Request ID ▾ contains ▾ Show 20 ▾ records

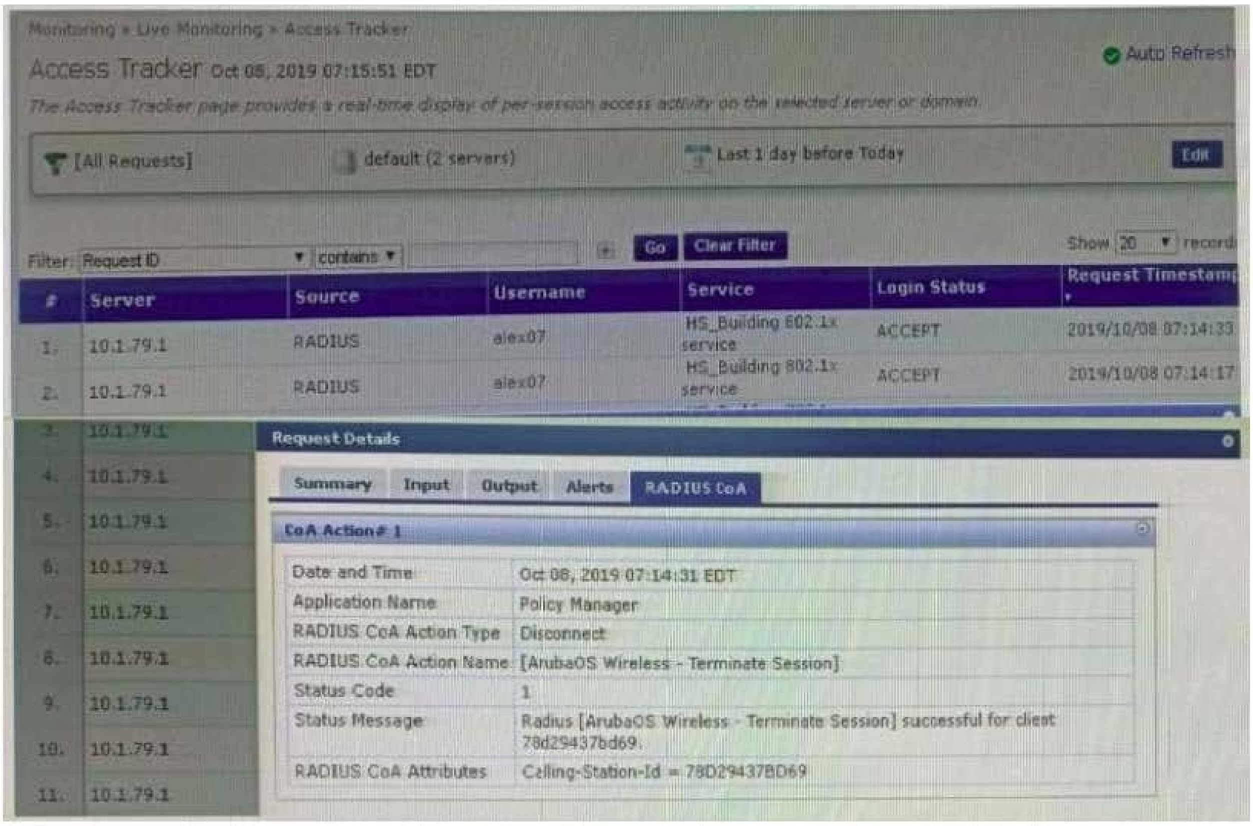
#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	10.1.79.1	RADIUS	alex07	HS_Building 802.1x service	ACCEPT	2019/10/08 07:14:33
2.	10.					10/08 07:14:17
3.	10.					10/08 07:11:32
4.	10.					10/08 07:10:11
5.	10.					10/08 07:09:01
6.	10.					10/08 07:07:58
7.	10.					10/08 07:03:48
8.	10.					10/08 07:02:36
9.	10.					10/08 02:27:58
10.	10.					10/07 14:27:58
11.	10.					10/07 13:44:03
12.	10.					10/07 12:55:42
13.	10.					10/07 12:51:53
14.	10.					10/07 12:50:59

Request Details

Login Status:	ACCEPT
Session Identifier:	R000001a8-01-5d9c6f99
Date and Time:	Oct 08, 2019 07:14:33 EDT
End-Host Identifier:	78D29437BD69 (Computer / Windows / Windows)
Username:	alex07
Access Device IP/Port:	10.1.70.100:0 (ArubaController / Aruba)
System Posture Status:	UNKNOWN (100)

Policies Used -	
Service:	HS_Building 802.1x service
Authentication Method:	EAP-PEAP
Authentication Source:	AD:AD1.aruba1.local
Authorization Source:	AD1, AD2, Corp SQL
Roles:	[Machine Authenticated], [User Authenticated]
Enforcement Profiles:	Aruba Limited Access for Profiling
Service Monitor Mode:	Disabled
Online Status:	Not Available

Showing 1 of 1-20 records



Monitoring » Live Monitoring » Access Tracker

Access Tracker Oct 08, 2019 07:15:51 EDT

The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

Filter: Request ID ▼ contains ▼

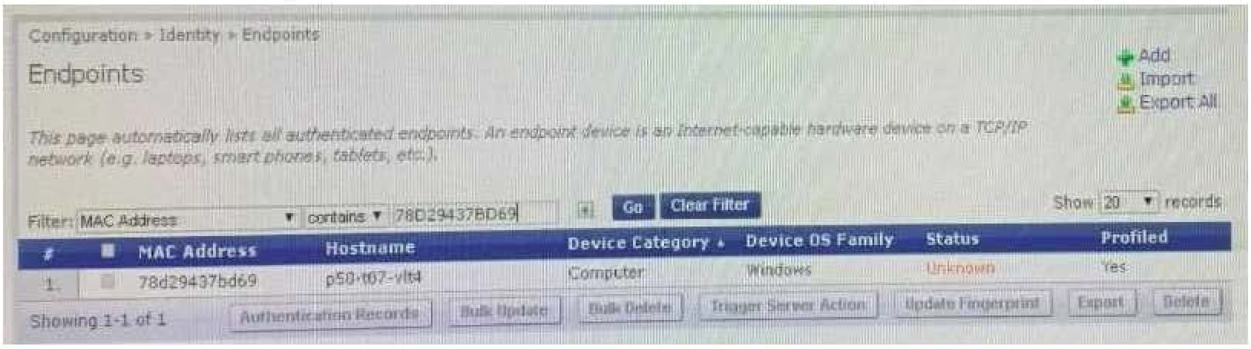
Show 20 ▼ record

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	10.1.79.1	RADIUS	alex07	HS_Building 802.1x service	ACCEPT	2019/10/08 07:14:33
2.	10.1.79.1	RADIUS	alex07	HS_Building 802.1x service	ACCEPT	2019/10/08 07:14:17
3.	10.1.79.1					
4.	10.1.79.1					
5.	10.1.79.1					
6.	10.1.79.1					
7.	10.1.79.1					
8.	10.1.79.1					
9.	10.1.79.1					
10.	10.1.79.1					
11.	10.1.79.1					

Request Details

CoA Action# 1

Date and Time	Oct 08, 2019 07:14:31 EDT
Application Name	Policy Manager
RADIUS CoA Action Type	Disconnect
RADIUS CoA Action Name	[ArubaOS Wireless - Terminate Session]
Status Code	1
Status Message	Radius [ArubaOS Wireless - Terminate Session] successful for client 78d29437bd69.
RADIUS CoA Attributes	Calling-Station-Id = 78D29437BD69



Configuration » Identity » Endpoints

Endpoints

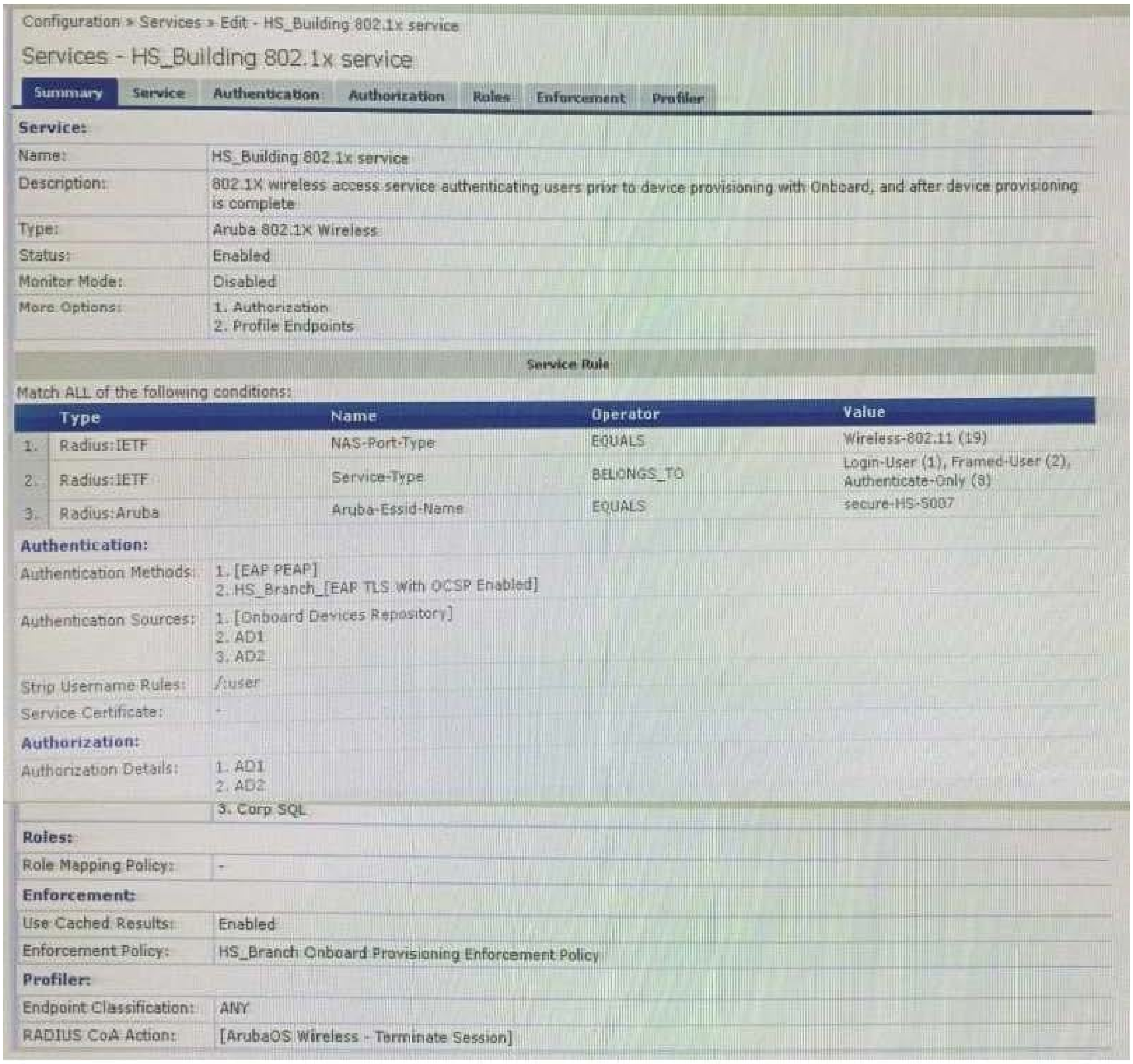
This page automatically lists all authenticated endpoints. An endpoint device is an Internet-capable hardware device on a TCP/IP network (e.g. laptops, smart phones, tablets, etc.).

Filter: MAC Address ▼ contains ▼ 78D29437BD69

Show 20 ▼ records

#	■	MAC Address	Hostname	Device Category	Device OS Family	Status	Profiled
1.	□	78d29437bd69	p50-t07-vlt4	Computer	Windows	Unknown	Yes

Showing 1-1 of 1


Configuration » Services » Edit - HS_Building 802.1x service
Services - HS_Building 802.1x service
Summary
Service
Authentication
Authorization
Roles
Enforcement
Profiler

Service:

Name:	HS_Building 802.1x service
Description:	802.1X wireless access service authenticating users prior to device provisioning with Onboard, and after device provisioning is complete
Type:	Aruba 802.1X Wireless
Status:	Enabled
Monitor Mode:	Disabled
More Options:	1. Authorization 2. Profile Endpoints

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3.	Radius:Aruba	Aruba-Essid-Name	EQUALS	secure-HS-5007

Authentication:

Authentication Methods:	1. [EAP PEAP] 2. HS_Branch_[EAP TLS With OCSP Enabled]
Authentication Sources:	1. [Onboard Devices Repository] 2. AD1 3. AD2
Strip Username Rules:	/:user
Service Certificate:	-

Authorization:

Authorization Details:	1. AD1 2. AD2 3. Corp SQL

Roles:

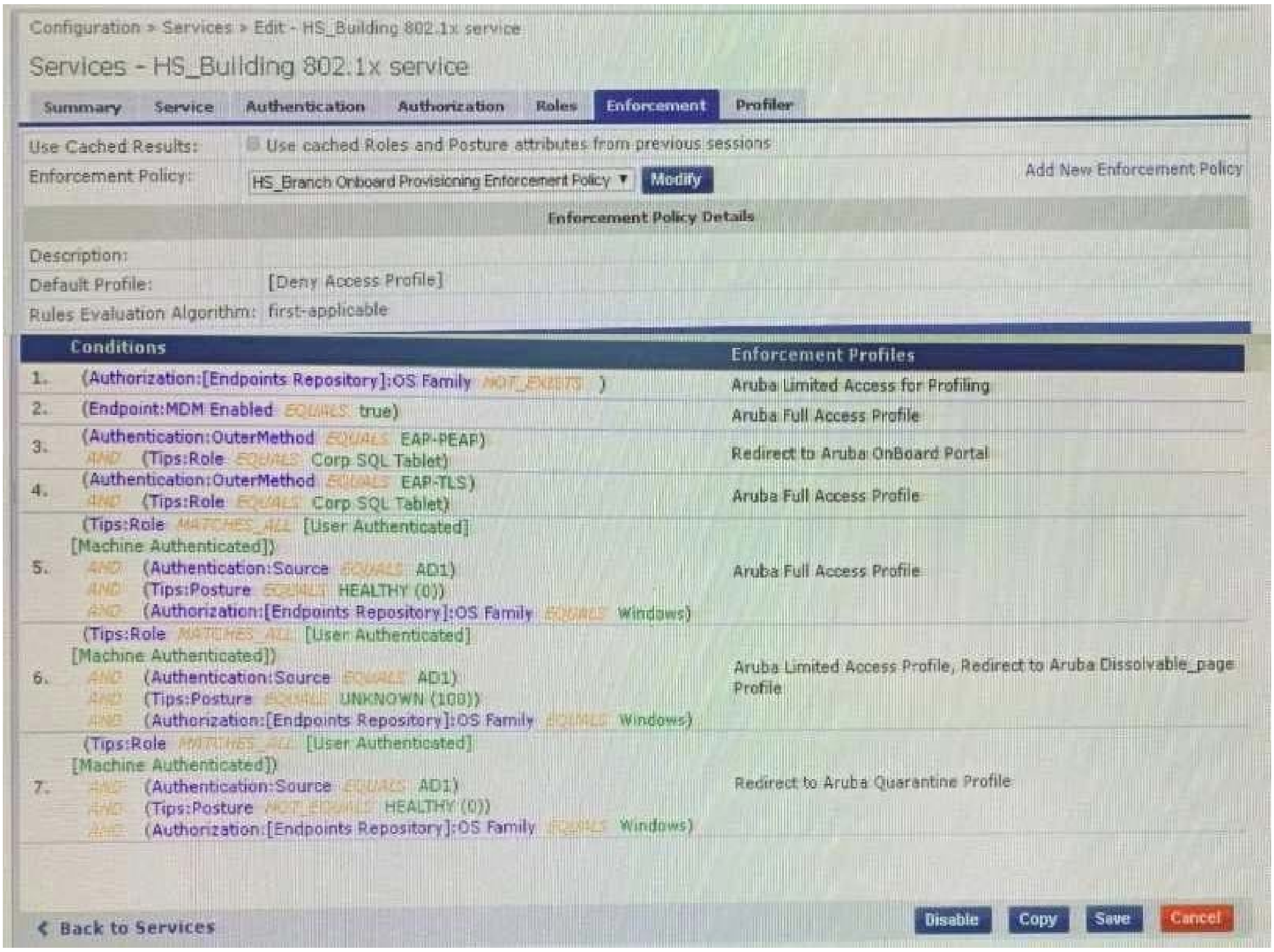
Role Mapping Policy:	-

Enforcement:

Use Cached Results:	Enabled
Enforcement Policy:	HS_Branch Onboard Provisioning Enforcement Policy

Profiler:

Endpoint Classification:	ANY
RADIUS CoA Action:	[ArubaOS Wireless - Terminate Session]



Services - HS_Building 802.1x service

Use Cached Results: □ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: HS_Branch Onboard Provisioning Enforcement Policy ▼

Enforcement Policy Details

Description:

Default Profile: [Deny Access Profile]

Rules Evaluation Algorithm: first-applicable

	Conditions	Enforcement Profiles
1.	(Authorization:[Endpoints Repository]:OS Family NOT_EXISTS)	Aruba Limited Access for Profiling
2.	(Endpoint:MDM Enabled EQUALS true)	Aruba Full Access Profile
3.	(Authentication:OuterMethod EQUALS EAP-PEAP) AND (Tips:Role EQUALS Corp SQL Tablet)	Redirect to Aruba OnBoard Portal
4.	(Authentication:OuterMethod EQUALS EAP-TLS) AND (Tips:Role EQUALS Corp SQL Tablet)	Aruba Full Access Profile
5.	(Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture EQUALS HEALTHY (0)) AND (Authorization:[Endpoints Repository]:OS Family EQUALS Windows)	Aruba Full Access Profile
6.	(Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture EQUALS UNKNOWN (100)) AND (Authorization:[Endpoints Repository]:OS Family EQUALS Windows)	Aruba Limited Access Profile, Redirect to Aruba Dissolvable_page Profile
7.	(Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture NOT_EQUALS HEALTHY (0)) AND (Authorization:[Endpoints Repository]:OS Family EQUALS Windows)	Redirect to Aruba Quarantine Profile

You configured the 802 1 x service enforcement conditions with the Endpoint profiling data. When the client connects to the network. ClearPass successfully profiles the client but the client always receives an incorrect enforcement profile The configurations in the Aruba controller are completed correctly. What is the cause of the issue?

A. An additional authorization source should be configured for profiling to work.

B. The enforcement policy conditions configured with profiling data are not correct.

C. The enforcement policy rules evaluation algorithm Is not configured correctly.

D. The option, use cached roles and posture from previous sessions should be enabled.

Correct Answer: B

HPE6-A81 PDF Dumps HPE6-A81 VCE Dumps HPE6-A81 Exam Questions